CLAIMS

1.- A method (100) for defining a filtering module (5) suitable for filtering information, according to a predetermined security policy, between a first module (2) adapted for processing information with a first sensitivity level, and a second module (3) adapted for processing information with a second sensitivity level distinct from the first sensitivity level, said first and second modules being connected, in parallel with the filtering module, by a cryptographic module (4) suitable for applying cryptographic functions, the method being characterized in that it comprises the following steps:

- a set of filtering rules is defined (101), translating the predetermined security policy, in a compilablelanguage, said filtering rules defining the properties of the information whereof transmission is allowed by the filtering module (5) between the first and second modules;
- validation processing for the predefined set of rules is carried out (102), validating that a transmission authorization or refusal has in fact been provided by applying said set of rules to any information that may be provided at the input of the filtering module;
- said predefined set of rules is compiled (103);
- said compiled set of rules is integrated into a rules database (15) of the filtering module.

2.- The method for defining a filtering module (5) according to claim 1, wherein the set of filtering rules defines static, time and dynamic properties of the information authorized to be transmitted.

3.- The method for defining a filtering module (5) according to claim 1 or 2, wherein the set of filtering rules includes at least one protocol automaton, defined by a set of states corresponding to successive steps of the implementation of a communication protocol, and events causing transitions between said states.

4.- The method for defining a filtering module (5) according to any one of the preceding claims, wherein the filtering module includes a processing module (14) adapted for executing all of the rules integrated into the rules database (15) upon receipt of information to be filtered and adapted for allowing or refusing transmission by the filtering module of said information between the first (2) and second (3) modules according to a refusal or an authorization provided following the execution of said set of rules.

5.- The method for defining a filtering module (5) according to claim 4, wherein state variables (16) associated with the filtering rules are defined, and a refusal or authorization

is provided following the execution of said set of rules as a function of current values calculated for said state variable values.

6.- The method for defining a filtering module (5) according to any one of the preceding claims, wherein the validation processing for the predefined set of rules further comprises a step for validating the coherence of the rules of said set of rules.

7.- The method for defining a filtering module (5) according to claim 6, wherein the step for validating the coherence of the rules comprises detecting at least one anomaly from among:

- the existence in the set of rules of first and second rules associated with different actions, the first rule being applied on all of the objects of the second;
- the existence in the set of rules of two rules associated with different actions, and each of them is applied on a subset of the objects to which the other is applied;
- the existence of two rules executing the same action on the same objects

8.- The method for defining a filtering module (5) according to any one of the preceding claims, wherein the set of rules is defined according to a rules tree structure.

9.- The method for defining a filtering module (5) according to any one of the preceding claims, wherein the filtering module is defined such that the information from the first module (2) whereof transmission is authorized by the filtering module is transmitted to the second module (3) in clear.

10.- The method for defining a filtering module (5) according to any one of the preceding claims, wherein the application order and logic composition of the results of the rules is defined by the set of filtering rules.

11.- A filtering module (5) suitable for filtering information according to a security policy between a first module (2) adapted for processing sensitive information, and a second module (3) adapted for processing non-sensitive information, said first and second modules being connected, in parallel with the filtering module, by a cryptographic module (4) suitable for applying cryptographic functions,
said filtering module being characterized in that it comprises a processing module (14) and a rules database (15) including a set of rules defining the predetermined security policy, in a compiled language, said filtering rules defining the properties of the information

whereof transmission is authorized by the filtering module (5) between the first and second modules.

12.- The filtering module according to claim 11, wherein the set of rules integrated into the rules database results from a method according to one of claims 1 to 10.

13.- Cryptographic equipment including:

- a first module (2) adapted for processing information with a first sensitivity level;
- a second module (3) adapted for processing information with a second sensitivity level different from the first sensitivity level;
- a cryptographic module (4) suitable for applying cryptographic functions, connecting said first and second modules;
- a filtering module (5) according to one of claims 11 to 12, suitable for filtering information according to a security policy between the first module (2) and the second module (3).

CLAIMS

1. A method (100) for defining a filtering module (5) suitable for filtering information, according to a predetermined security policy, between a first module (2) adapted for processing information with a first sensitivity level, and a second module (3) adapted for processing information with a second sensitivity level distinct from the first sensitivity level, said first and second modules being connected, in parallel with the filtering module, by a cryptographic module (4) suitable for applying cryptographic functions, the method being characterized in that it comprises the following steps:

- a set of filtering rules is defined (101), translating the predetermined security policy, in a compilable language, said filtering rules defining the properties of the information whereof transmission is allowed by the filtering module (5) between the first and second modules; and

wherein the set of filtering rules includes at least one protocol automaton, defined by a set of states corresponding to successive steps of the implementation of a communication protocol, and events causing transitions between said states;

- validation processing for the predefined set of rules is carried out (102), validating that a transmission authorization or refusal has in fact been provided by applying said set of rules to any information that may be provided at the input of the filtering module;

- said predefined set of rules is compiled (103);

- said compiled set of rules is integrated into a rules database (15) of the filtering module.

2. The method for defining a filtering module (5) according to claim 1, wherein the set of filtering rules defines static, time and dynamic properties of the information authorized to be transmitted.

3. The method for defining a filtering module (5) according to any one of the preceding claims, wherein the filtering module includes a processing module (14) adapted for executing all of the rules integrated into the rules database (15) upon receipt of information to be filtered and adapted for allowing or refusing transmission by the filtering module of said information between the first (2) and second (3) modules according to a refusal or an authorization provided following the execution of said set of rules.

4. The method for defining a filtering module (5) according to claim 3, wherein state variables (16) associated with the filtering rules are defined, and a refusal or authorization is provided following the execution of said set of rules as a function of current values calculated for said state variable values.

5. The method for defining a filtering module (5) according to any one of the preceding claims, wherein the validation processing for the predefined set of rules further comprises a step for validating the coherence of the rules of said set of rules.

6. The method for defining a filtering module (5) according to claim 5, wherein the step for validating the coherence of the rules comprises detecting at least one anomaly from among:

- the existence in the set of rules of first and second rules associated with different actions, the first rule being applied on all of the objects of the second;

- the existence in the set of rules of two rules associated with different actions, and each of them is applied on a subset of the objects to which the other is applied;

- the existence of two rules executing the same action on the same objects

7. The method for defining a filtering module (5) according to any one of the preceding claims, wherein the set of rules is defined according to a rules tree structure.

8. The method for defining a filtering module (5) according to any one of the preceding claims, wherein the filtering module is defined such that the information from the first module (2) whereof transmission is authorized by the filtering module is transmitted to the second module (3) in clear.

9. The method for defining a filtering module (5) according to any one of the preceding claims, wherein the application order and logic composition of the results of the rules is defined by the set of filtering rules.

10. A filtering module (5) suitable for filtering information according to a security policy between a first module (2) adapted for processing sensitive information, and a second module (3) adapted for processing non-sensitive information, said first and second modules being connected, in parallel with the filtering module, by a cryptographic module (4) suitable for applying cryptographic functions,

said filtering module being characterized in that it comprises a processing module (14) and a rules database (15) including a set of rules defining the predetermined security policy, in a compiled language, said filtering rules defining the properties of the information whereof transmission is authorized by the filtering module (5) between the first and second modules and

wherein the set of rules integrated into the rules database results from a method according to one of claims 1 to 9.

11. Cryptographic equipment including:

- a first module (2) adapted for processing information with a first sensitivity level;

- a second module (3) adapted for processing information with a second sensitivity level different from the first sensitivity level;

- a cryptographic module (4) suitable for applying cryptographic functions, connecting said first and second modules;

- a filtering module (5) according to claim 10, suitable for filtering information according to a security policy between the first module (2) and the second module (3).